CLAIMS:

1.   A method of operating a data-processing device, particularly a chip card or smart card, with an integrated circuit comprising a central processing unit (CPU) and one or more co-processors, in which the integrated circuit performs cryptographic operations, characterized in that in performing a cryptographic operation in the integrated circuit, at least

5   two processors, CPU and co-processors, perform a cryptographic operation simultaneously and in parallel.

2.   A method as claimed in claim 1, characterized in that only the cryptographic operation of one processor, CPU or co-processor, is a useful operation and all other

10   cryptographic operations are dummy operations whose results are rejected.

3.   A method as claimed in claim 2, characterized in that the selection as to which processor, CPU or co-processor, performs a useful operation is random-controlled.

15   4.   A method as claimed in any one of the preceding claims, characterized in that a cryptographic operation is split up into at least two sub-operations and in that at least two processors perform the sub-operations in parallel and simultaneously.

5.   A method as claimed in claim 4, characterized in that, in the sense of current

20   consumption, a cryptographic operation is split up into two mutually complementary operations.

6.   A method as claimed in claim 5, characterized in that the selection as to which processor performs the operation complementarily or not complementarily is random-

25   controlled.

7.   A method as claimed in claim 1, characterized in that a cryptographic operation is split up into at least two sub-operations, and the sub-operations are performed simultaneously and in parallel by the processors, CPU and co-processors, while subsequently

corresponding sub-results are combined to an overall result of the overall cryptographic operation.

8.   A method as claimed in claim 7, characterized in that the split-up of the
5   cryptographic operation into sub-operations is random-controlled.

9.   A method as claimed in claim 7 or 8, characterized in that the sub-operations are parts of an encryption in accordance with DES (Data Encryption Standard).

10   10.   A data-processing device, particularly a chip card or smart card, particularly for performing a method as claimed in any one of the preceding claims, with an integrated circuit comprising a central processing unit (CPU) (10) and one or more co-processors (12), characterized in that the integrated circuit comprises a control unit (18, 30) which controls the processors, CPU (10) and co-processors (12) in such a way that, in the case of a
15   cryptographic operation, at least two processors perform a cryptographic operation simultaneously and in parallel.

11.   A data-processing device as claimed in claim 10, characterized in that the control unit comprises a splitter (18) which splits up a cryptographic operation into at least
20   two sub-operations (20, 22) and supplies them for simultaneous processing to two separate processors of the integrated circuit, CPU (10) and co-processors (12).

12.   A data-processing device as claimed in claim 11, characterized in that the control unit further comprises a recombiner (30) which recombines each sub-result (26, 28)
25   of the sub-operations (20, 22) simultaneously performed by the processors (10, 12).

13.   A data-processing device as claimed in claim 12, characterized in that the splitter (18) is formed in such a way that at least one sub-operation (20, 22) is a dummy operation and in that the recombiner (30) is formed in such a way that it rejects the relevant
30   result (26, 28) of a processor (10, 12) that has performed a dummy operation.

14.   A data-processing device as claimed in any one of claims 11 to 13, characterized in that the integrated circuit additionally comprises a random generator (24)

which is connected to the splitter (18) in such a way that it operates in a random-controlled manner.

LIST OF REFERENCE SIGNS

	10	central processing unit (CPU)
	12	co-processor
5	14	data input
	16	data output
	18	splitter
	20	first data part
	22	second data part
10	24	random input
	26	first result
	28	second result
	30	recombiner
	32	connection between splitter and recombiner
15	34	time axis